Reclamation Manual

Directives and Standards

Subject: Reclamation Information Technology (IT) Security Program: Information/Data Security

Purpose: Defines and establishes the responsibilities and procedures required to safeguard Reclamation's information/data.

Authority: The Privacy Act of 1974 (5 U.S.C. § 552a); Federal Managers' Financial Integrity Act of 1983 (Public Law 97-255); Office of Management and Budget (OMB) Circular No. A-123, *Management Accountability and Control* (31 U.S.C. § 3512, June 21, 1995); The Computer Security Act of 1987 (Public Law 100-235); Fiscal Year 2001 Defense Authorization Act (Public Law 106-398) including Title X, Subtitle G, *Government Information Security Reform*; OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Systems* (50 Federal Register 52730, December 24, 1985); *Practices for Securing Critical Information Assets*, Critical Infrastructure Assurance Office (CIAO) (January 2000); Department of the Interior Departmental Manual (DM) Part 375, Chapter 19, *Information Technology Security*; Federal Records Act of 1950, as amended (44 U.S.C. § 2107); Freedom of Information Act, as amended (5 U.S.C. § 552); Information Technology Management Reform Act of 1996 (40 U.S.C. § 1401); Presidential Decision Directive 63, *National Critical Infrastructure Protection*, May 1998; and Reclamation Manual (RM), *BOR Automated Information System (AIS) Security,* IRM 08-01.

Contact: Information Technology Services Division, D-7100
Property and Office Services Division, D-7900

1. **Introduction.** Electronic information/data are managed and protected as a Reclamation-wide asset. This Directive and Standard defines categories of information/data for the purposes of security and management, describes the processes for accessing information/data from both internal or external sources, and details the necessary protective procedures.

2. **Goal.** To protect and manage information/data from unauthorized disclosure, compromise, or alteration and to ensure availability for authorized purposes.

3. **Definitions.**

   A. **Restricted.** Information/data, including that received from external sources, requiring the highest level of *Access Control* protections based on the extent of harm caused by its unauthorized, inadvertent, or deliberate disclosure, alteration, use, or destruction. Such improper use, modification, or disclosure would adversely affect Reclamation's business partners, customers, and employees and the agency's ability to accomplish its

mission, safeguard the public, and protect the legal and financial rights of the Government.

B. **Sensitive.** Information/data for internal use only by authorized Reclamation employees, business partners, and customers through established *Access Controls*. The unauthorized, inadvertent, or deliberate disclosure, alteration, use, or destruction of such information/data could affect Reclamation's ability to perform agency functions, impede daily business activities, and/or affect employee productivity. Release to the public requires prior approval from the Director, or designee, who has responsibility for the IT system.

C. **Public.** Read-Only information/data made available for public disclosure through the Internet, publication, or other distribution. *Access Controls* are incorporated to prevent the modification or deletion of information/data residing in Reclamation systems.

D. **Authorized Access.** The level of information/data access which has been granted through a determination of *Need to Know.*

E. **Need to Know.** The formal process of determining one's *Authorized Access* or need to read, create, modify, or disclose information/data for legitimate business purposes in the course of daily Government activities.

F. **Access Control.** Protection of information/data through the use of passwords, call-back devices, encryption, data authentication, security software, and other appropriate methods to prevent access and/or the unauthorized use, modification, or disclosure of information/data on computers, peripheral devices, storage media, or transmitted over Reclamation networks.

G. **Public Access**. The ability of the public to readily access and obtain Reclamation information/data.

4. **Scope.** This Directive and Standard applies to Reclamation information/data accessed by employees, contractors, consultants, volunteers, and the public.

5. **Procedures.**

A. **Information/Data Access Controls.**

(1) **Restricted.**

(a) Information/data will not be accessible via any form of hyper-link to the Internet or Intranet unless strong authentication is implemented across the

perimeter or security zone. (See RM, *Reclamation InformationTechnology Security Program: Network Systems*, IRM 08-02.) *Authorized Access* to these systems will be limited by the highest levels of *Access Controls* and an established *Need to Know*.

(b) Information/data converted to hardcopy will be maintained in locked cabinets, in secure areas, and access will require a *Need to Know* determination by the Director, or designee, who has responsibility for the IT system. When not in immediate use, all hardcopy documents containing restricted information/data will be maintained in locked cabinets.

(c) Information/data, in either electronic or hardcopy format, cannot be released to the public, except with a demonstrated *Need to Know* and prior approval by the Director, or designee, who has responsibility for the IT system.

(2) **Sensitive.** Information/data are available for internal use only by authorized Reclamation employees, contractors, business partners, and customers. Public access to "read only" information/data may be granted with a demonstrated *Need to Know* and prior approval by the Director, or designee, who has responsibility for the IT system. Monitoring of electronic systems is required to ensure accuracy, completeness, and reliability of information/data.

(3) **Public.** There are no *Access Controls* required for this information/data, and its disclosure will cause no harm regarding Reclamation's ability to conduct the public's business or impede its mission-related activities. Public use of this information/data is in "Read-Only" format from the Internet. Data integrity will be ensured through monitoring, regular updates, and comparison to securely stored replication data. There are no special physical security restrictions on hardcopy documents.

B. **Transmission Controls.** Transmission of electronic information/data will occur only with the use of established network *Access Controls* to prevent possible modification or disclosure.

C. **Reproduction, FAX, and Transfer Controls.**

(1) **Restricted.** Information/data in this category requires the recipient's *Need to Know* to be established and high-level *Access Controls* to be in place. *Authorized Access* is granted by the Director, or designee, who has responsibility for the IT system, and authorized personnel control the entire reproduction/transfer process. All copies, reproductions, or media transfers must be documented, and all hardcopies, reproductions, and media must be maintained in locked cabinets in

restricted areas. Electronic copies of restricted documents must be encrypted when they are transferred.

(2) **Sensitive.** Information/data in this category also requires the recipient's *Need to Know* to be established and normal *Access Controls* to be in place. *Authorized Access* must be granted and all copies, reproductions, or media transfers must be approved. Electronic copies of sensitive documents will be encrypted when they are transferred.

(3) **Public.** No restrictions on copies, reproductions, or media transfers for information/data in this category.

D. **Labeling and Reporting.**

(1) All IT systems will have the data storage media labeled with the highest level of sensitivity which may be found on the systems, e.g., *Restricted, Sensitive,* or *Public*. Any changes which may affect the level of security handled by the system or security operational controls will be reported to the local IT Security Manager, the system's owner, and the office manager.

(2) Restricted and sensitive documents in both electronic and hardcopy will be labeled *"Restricted"* or *"Sensitive"* as a header or footer on every page. An orange Security Sensitive cover sheet will be attached to paper copies of restricted documents.

6. **Responsibilities.**

A. **Chief Information Officer (CIO).** The CIO has overall responsibility for the IT Security Program in Reclamation.

B. **Directors of Reclamation Regions and Offices.** Directors of Reclamation Regions and Offices have responsibility for the security of the IT systems under their authority. This responsibility may be delegated no more than one level down (Deputy or Assistant Directors). As system owners, they are responsible for ensuring the proper use of information/data related to their systems, including:

(1) Conducting risk assessments and approving information/data classifications in the IT system security plan;

(2) Implementing appropriate administrative, operational, and disposal procedures to safeguard information/data in compliance with IT and records management policies, directives, and standards;

(3) Granting access in accordance with established standards; and

(4) Incorporating records management and IT security standards into systems development, operations, and maintenance practices.

C. **Reclamation's Regional Information Technology Security Managers (ITSMs).** ITSMs support the formation and coordination of processes to ensure information/data security is adequate, appropriate, and supports Reclamation-wide IT security policy, and directives and standards. The ITSMs ensure compliance with information/data security restrictions and requirements. The Bureau ITSM coordinates with the ITSMs and acts as liaison to the Manager, Information Technology Services Division, or the CIO as appropriate.

D. **Reclamation Employees, Contractors, Consultants, and Volunteers.** Reclamation employees, contractors, consultants, and volunteers including external parties, are responsible for compliance with this Directive and Standard. Government employees who willingly and deliberately violate this Directive and Standard will be subject to disciplinary action.

7. **Related Directives and Standards.** Related Directives and Standards are found in the Information Resources Management (IRM) section of the RM.